Section IV: **Network Security**
Title: **Network Architecture Security Standard**
Current Effective Date: **June 30, 2008**
Revision History: **May 7, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To ensure the confidentiality, integrity, and availability of data within the North Carolina (NC) Department of Health and Human Services (DHHS) data and telecommunication networks.

STANDARD

1.0 Background

The Divisions and Offices shall take a proactive approach to managing their data and telecommunication network. It may be necessary for the Divisions and Offices to supplement the standards herein with additional measures for safeguarding their information as required to meet their organization requirements.

The DHHS acknowledges that some of the Divisions and Offices do not directly create, control, and/or maintain their data resources or telecommunication network. In this instance, the Division Information Security Official (ISO) shall ensure there is a service level agreement (SLA) with the service provider and that the SLA requires the service provider to comply with all applicable policies, standards, and guidelines.

2.0 Physical Controls

All data, telecommunication network, and related equipment (e.g., network patch panels, switches, hubs, management consoles, dumb terminals, and/or any other active/passive components, etc.) shall comply with the NC DHHS Security Standards, Physical Security Standards – Site Security Plan Standard.

Any unused network ports shall be logically secured to ensure that all network/workstation ports are re-assigned or disabled at the switch/router level. In addition, all network/workstation ports that are re-assigned and disabled should be documented.

3.0 Network Perimeter

All network points of ingress and egress between entities outside the DHHS network and the Divisions and Offices shall terminate within the Enterprise Services Access Point (ESAP), which serves as the DHHS virtual data network perimeter.

4.0 Logical Controls

Logical access to network management and network configuration facilities shall be strictly controlled by the Division ISO. All network diagnostic, testing, and monitoring equipment must be accessible and used only under strict managerial control by qualified staff. All software and hardware maintenance procedures and contracts shall be fully documented. Mechanisms that provide early warning of potential problems with network hardware shall be implemented and monitored at all times. The logical access controls (e.g., user name and password) shall be changed from the default values.

The Division ISO shall approve network services and protocols that are implemented on their devices. All other protocols and services will be removed and/or disabled. Network port assignments and re-assignments must be logged, managed, secured, and documented.

5.0 Business Continuity Plan (BCP)

Redundancy shall be considered for the network architecture using the DHHS Business Impact Analysis (BIA) to determine availability of critical data in case of catastrophic failure of network components. The redundancy shall be formulated and based on pre-determined severity levels of the BIA acceptable to the Division and Office. These redundancy measures must be specified in any SLAs with any service provider and each SLA must reflect desired availability.

All critical network hardware (e.g., networking and telecommunication) components must operate from an uninterruptible power supply (UPS) system in conjunction with backup power supply (e.g., generators, etc.). The recovery of the network should be included in a formal contingency plan or Business Continuity Plan (BCP), which should be tested on a regular basis.

6.0 Workstations

All workstations will be secured in accordance with the NC State Office of Information Technology Services (ITS) Security Manual – Statewide Information Technology Standard, the NC DHHS Security Standards, Application Security Standards – User Authorization and Authentication Standard and the NC DHHS Security Standards, Physical Security Standards – Asset Inventory and Control Standard.

7.0 Content Filtering

In order to prevent workforce members from accessing inappropriate Internet sites and materials, the Divisions and Offices shall comply with the NC State Office of Information Technology Services (ITS) Security Manual – Statewide Information Technology Standard.

8.0 Data Integrity

In order to maintain the integrity of data (both in transit and at rest) it is recommended that encryption be used, as specified in the NC DHHS Security Standards, Network Security Standards – Encryption Security Standard.

9.0 Network Addressing

All network names and addresses shall be managed and approved by the Division of Information Resource Management (DIRM), which is the central addressing authority within DHHS.

10.0 Intrusion Detection and Prevention

The DHHS Privacy and Security Office (PSO) shall implement and manage an intrusion detection and prevention system and/or process for the Department under Enterprise Services Access Point (ESAP).

The DHHS PSO shall work with the Divisions and Offices, through the Division ISO, to implement any applicable local intrusion detection and prevention system and/or process. The DHHS PSO will work with the Division ISO to schedule and perform data network vulnerability and penetration testing.

11.0 Documentation

The Divisions and Offices shall maintain current DHHS network diagrams (e.g., devices, locations, physical connections, configurations, etc.). All devices connected to the DHHS network must be registered and all modifications to the DHHS network, unless unauthorized activity is suspected or detected, must be approved and reflected in the DHHS network diagram by the Division ISO prior to implementation. Modifications should be executed during an established maintenance window. The Division ISO shall ensure that all changes to the DHHS network meet at least the following criteria:

- That the updates are necessary
- That they do not conflict with other network functionality
- That they do not compromise the network security
- That they are never performed on systems while they are in a production state (excluding those taken for security issues as addressed above)
- That they are completed in accordance with the manufacturer's recommendations

If unauthorized activity is suspected or detected, every effort shall be made to immediately isolate the device in question and trace it to a physical location. This shall be reported as an incident per the NC DHHS Security Standards, Administrative Security Standards – Incident Management and Response Security Standard. This is the only exception to prior approval, as stated in the previous paragraph, and the Division ISO must be notified of the changes to mitigate the incident within one (1) business day.

The Division ISO shall strictly control all access to the DHHS network diagrams. All requests for the DHHS network diagrams must be submitted to the Division ISO in writing, prior to granting access, authorization, and approval.

12.0 Compliance Review

Each DHHS Division and Office shall review all governing policies, procedures, standards, laws, and regulatory compliance mandates in coordination with the DHHS PSO on a regular basis (recommended annually). Any gaps and deficiencies revealed by the review shall be remediated as soon as possible, and no later than the next review.

References:

- DHHS Directive Number II-12: Delegation of Authority to the Director, Division of Information Resource Management (DIRM)

- NC State Office of Information Technology Services (ITS) – Enterprise Services Access Point (ESAP)

- NC State Office of Information Technology Services (ITS) Security Manual – Statewide Information Technology Standard

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 2 – Controlling Access to Information and Systems – Section 01: Controlling Access to Information and Systems
    - Standard 020103 – Securing Unattended Work Stations
    - Standard 020106 – Managing Passwords
  - Chapter 3 – Processing Information and Documents – Section 01: Networks
    - Standard 030101 – Configuring Networks
    - Standard 030102 – Managing the Networks
    - Standard 030105 – Network Segregation

- NC DHHS Security Standards
  - Administrative Security Standards
    - Incident Management and Response Security Standard
    - Information Security Risk Management Standard
  - Application Security Standards
    - User Authorization and Authentication Standard
  - Network Security Standards
    - Digital Signatures Security Standard
    - Encryption Security Standard
    - Network Security and Firewalls Standard
    - Telecommunication Security Standard
    - User Authorization and Authentication Standard
    - Wireless Security Standard

- Physical Security Standards
  - Asset Inventory and Control Standard
  - Site Security Plan Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - Business Continuity and Disaster Recovery Plan(s) Policy
  - Data Protection Policy
  - ITS Operations Security Policy
  - Network and Telecommunication Security Policy
  - Wireless Security Policy